Creating an IA Empowered Workforce – Standardizing Skill Development

By Sandra J. Smith

The Department of Defense Directive (DoDD) 8570.1, Information Assurance (IA) Training, Certification, and Workforce Management, calls for further professionalization of the IA workforce. This instruction forever changes the way we identify, train, certify and assign personnel, who perform IA functions associated with managing and supporting DoD enclaves, networks and computing environments.

> *The protection of the GIG is everyone's business – this cannot be overstated. We take specific actions to train, license, qualify, and certify pilots and weapon systems users – we must consider no less of a standard for the operation, security, and integrity of the GIG. Our information base and our ability to leverage the technology to support warfighting, intelligence, and business functions must have the highest level of trust and confidence or we lose the advantage that information provides us.*
>
> *– Excerpts from Mission Possible - Security to the Edge*

The IA Imperative

Trusted information is the key to modern warfighting, and a secured Global Information Grid (GIG) is the cornerstone of this process. FORCEnet is the naval component of the GIG that will provide seamless and secure interoperability to Sailors, Marines and civilians. Since threats to information security can be catastrophic, our information must be protected from enemies, criminals, insiders or self-inflicted accidental events. Strong IA provides user confidence in information because the five crucial conditions — confidentiality, integrity, availability, authentication and non-repudiation — have been met. Creating a highly skilled and certified IA workforce becomes an imperative.

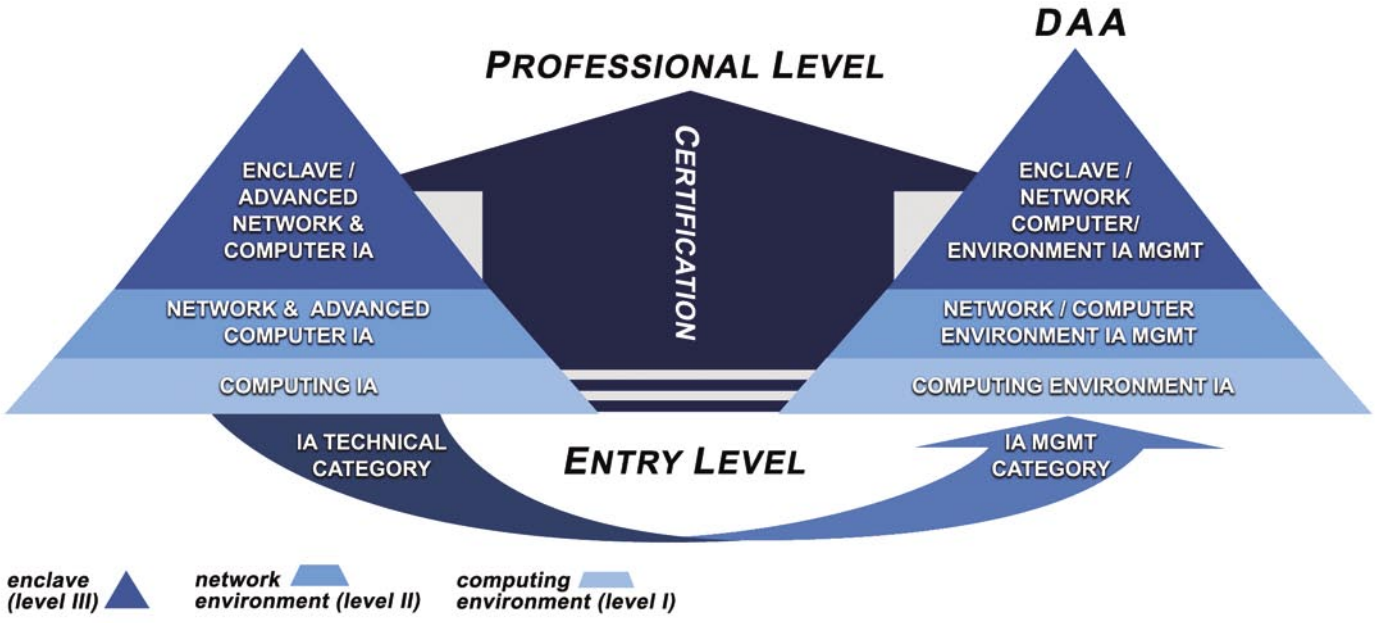
A Trained, Certified and Managed IA Workforce

Several DoD directives and instructions have been published over the last few years that provide high-level IA policies and responsibilities. By law, the DoD is required to ensure its workforce is sufficiently educated and trained to assure the security of government networks. Additionally, the Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (PL 107-347), requires the Department of the Navy (DON) to report to DoD on IA training statistics and the status of personnel performing IA functions.

DoDD 8570.1 specifically establishes IA training, certification and a workforce management policy for the Department of Defense, and authorizes publication of a manual that defines job role functions, minimum certification requirements and reporting, aligned to a four-year implementation plan. The focus of DoDD 8570.1 is on personnel (military, civilian, contractors and foreign nationals) with privileged access and IA managers.

The policy identifies IA personnel by the functions they perform — regardless of job series, occupational specialty or whether an

Figure 1. Proposed Overview of the IA Workforce Structure.



individual is full-time or assigned to an IA function as an additional duty. IA professionals working in policy or training areas that are not performing DoD-defined IA functions are not included as part of the IA workforce that requires certifications. The draft DoD 8570.1-M, currently being finalized by DoD, describes IA management and technical functions and IA workforce levels, as depicted in Figure 1. Key policy requirements include:

• All authorized users of DoD information systems (IS) shall receive initial IA awareness orientation as a condition of access and, thereafter, must complete annual IA refresher awareness.

• Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be properly identified in appropriate personnel databases.

• All positions involved in the performance of IA functions shall be identified in appropriate manpower databases by category and level.

• All IA personnel shall be identified, tracked and managed so that IA positions are staffed with personnel trained and certified by category, level and function.

• Privileged users and IA managers shall be fully qualified, trained and certified to DoD baseline requirements to perform their IA duties.

• The status of IA certification and training shall be monitored and reported as an element of mission readiness and as a management review item.

A DON Collaborative Approach

In response to these policy requirements, the DON IA Workforce Working Group (IAWWG) was established to help determine an Enterprise way ahead for implementation, and to develop strategies, recommendations and plans to achieve near- and long-term objectives. These objectives include standardizing skill development, ensuring blended and streamlined training, identifying associated efficiencies and identifying Naval Enterprise solutions to ensure compliance with workforce management mandates.

The DON CIO Strategy for Achieving Consistent IA Training, Certification, and Workforce Management, issued March 18, 2005, emphasizes key focus areas and an ongoing collaborative effort, which are crucial for not only achieving compliance, but also for strengthening the DON's IA posture, to grow and sustain a certified and trained IA workforce.

Under the auspices of the DON IAWWG, three tiger teams are focusing on (1) manpower and personnel; (2) training and certification; and (3) technological aspects of monitoring, tracking and reporting on the workforce. Initial efforts are focused on identifying personnel performing IA functions and improving records management of IA training. Identification of the workforce will also serve to establish a valid requirements baseline for human capital planning, and to formulate resource and implementation plans for IA training and certification programs.

The DoD's common naming schema will provide a universal language for delineating job roles of the IA workforce across the DON. Additional guidance will be provided as the IAWWG continues with Enterprise collaboration.

This is a major DON initiative that has engaged a dynamic group of representatives across the Department, which includes manpower, personnel and training organizations. As the DON further professionalizes the IA workforce with the knowledge, skills and tools to effectively prevent, deter and respond to threats, it not only shapes the workforce now and in the future, it ultimately supports network-centric operations and FORCEnet.

For additional information, visit the IA Workforce page of the DON CIO Web site at http://www.doncio.navy.mil/iaworkforce/.

Sandra J. Smith is the DON IM/IT Workforce Management team leader.

CHIPS

Annual IA Mandatory Training Deadline is Sept. 1, 2005 Do it: It's the Law!

All authorized users (military, civilians and contractors) of Department of Defense (DoD) information systems are required to complete information assurance (IA) awareness orientation training by Sept. 1, 2005.

IA awareness training is available for the Department of the Navy (DON) through Navy Knowledge Online (http://www.nko.navy.mil) and MarineNet (http://www.marinenet.usmc.mil). Depending on your organization's structure, the command information assurance manager (IAM), information assurance officer (IAO) or information systems security manager (ISSM) is responsible for ensuring that all personnel with active user accounts complete initial or refresher training.

The course takes about 30 minutes to complete and explains the importance of classified information and how to protect it from unauthorized users both inside and outside of the workplace. For more information and step-by-step instructions for accessing the IA training, please visit the IA workforce page of the DON CIO Web site at http://www.doncio.navy.mil/iaworkforce/. If you need additional assistance, please contact the following POCs:

Navy – (757) 417-6757/DSN 537-6757

Marine Corps – (703) 693-3490/DSN 223-3490

DON – (703) 601-0605/DSN 329-0605

CHIPS